This listing of claims will replace all prior versions, and listings, of claims in the application.

LISTING OF CLAIMS:

1. (Currently Amended) A method for communication via a computer network, the method comprising:

registering a plurality of users with a trusted body, including the steps of each of the users generating a first public/private key pair for a specific dialogue session, and sending the public key of the public/private key pair to the trusted body;

said trusted body verifying the identity of each user by using said public key;

said trusted body generating a random identifier for each user, and keeping a confidential record of the relation between the identity of each user and the random identifier for the user;

one of the users entering into a dialogue with one or more other users by sending messages over the computer network and through the trusted body to said one or more other users, wherein said one of the users remains anonymous through use of its random identifier until such time as the user reveals its identity to one or more of the other users; and

wherein the trusted body has a second public/private key pair, and the user encrypts said messages using the public key of said second public/private key pair, and the method includes said trusted body recording the dialogue by ~~encrypting each message of the dialogue using a second public key of a private key/public key pair of the trusted body~~ recording the encrypted messages, and using the recorded dialogue together with the confidential record of the relation between the identity of a user and the random identifier to provide a means of non-repudiation of the dialogue by users.

2. (Original) A method as claimed in claim 1, wherein the step of verifying the identity of a user is carried out by validating a public key cryptography certificate f or a user.

3. (Original) A method as claimed in claim 1, wherein the trusted body verifies the suitability of a user to participate in a dialogue.

4. (Original) A method as claimed in claim 1, wherein the trusted body verifies the authenticity of a message sent by a user.

5. (Original) A method as claimed in claim 4, wherein the trusted body uses public key cryptography to authenticate messages sent by a user.

6. (Original) A method as claimed in claim 1, wherein the trusted body time-stamps all messages from users when recording the dialogue formed by the messages between users.

7. (Original) A method as claimed in claim 1, wherein the dialogue is in real time.

8. (Original) A method as claimed in claim 1, wherein the trusted body prescribes a set of rules to be followed by the users.

9. (Previously Presented) A method as claimed in claim 1, wherein, the users can be any of individuals, corporate bodies, organizations, automated machines or software applications.

10. (Original) A method as claimed in claim 1, wherein a message from a user is sent to an input queue to ensure the correct order of the messages handled by the trusted body.

11. (Original) A method as claimed in claim 1, wherein messages can include attachments in the form of documents to be discussed in the dialogue between users.

12. (Original) A method as claimed in claim 11, wherein the attachments are signed or watermarked.

13. (Currently Amended) A system for communication via a computer network comprising:

a plurality of distributed computer systems connected by a computer network,

a trusted body connected to the computer network,

the trusted body including:

means for the trusted body to verify the identity of a user of a computer system by using said public key and means for generating a random identifier for a user, a record confidential to the trusted body of the relation between the identities of the users and the random identifiers;

means for two or more users to perform a dialogue by sending messages over the computer network and through the trusted body and to each other, wherein each user remains anonymous through use of its random identifier until such time as the user reveals its identity to one or more of the other users, and

wherein each of the users registers with the trusted body by generating a first public/private key pair for a specific dialogue session, and [[sends]] sending the public key of the public/private key pair to the trusted body, [[and]] the trusted body has a second public/private key pair, and the user encrypts said messages using the public key of said second public/private key pair, and said trusted body records the dialogue by ~~encrypting each message of the dialogue using a second public key of a private key/public key pair of the trusted body~~ recording the encrypted messages, and uses the recorded dialogue together with the confidential record of the relation between the identities of the users and the random identifiers to provide a means of non-repudiation of the dialogue by users.

14. (Original) A system as claimed in claim 13, wherein the computer network is the Internet and the trusted body is an Internet service provider.

15. (Original) A system as claimed in claim 13, wherein each user has a graphical user interface showing the dialogue and status of the other users.

16. (Original) A system as claimed in claim 15, wherein the graphical user interface includes a means for viewing a document sent by a user as an attachment to a message of the dialogue.

17. (Currently Amended) A computer program product stored on a computer readable storage medium, comprising computer readable program code means for performing the steps of:

registering a plurality of users with a trusted body, including the steps of each of the users generating a first public/private key pair for a specific dialogue session, and sending the public key of the public/private key pair to the trusted body;

said trusted body verifying the identity of each user by using said public key;

said trusted body generating a random identifier for each user, and keeping a confidential record of the relation between the identity of each user and the random identifier for the user;

wherein one of the users can enter into a dialogue with one or more other users by means of messages sent over the computer network and through the trusted body, wherein said one of

the users remains anonymous through use of its random identifier until such time as the user reveals its identity to one or more of the other users; and

wherein the trusted body has a second public/private key pair, and the user encrypts said messages using the public key of said second public/private key pair, and the method includes said trusted body recording the dialogue by ~~encrypting each message of the dialogue using a second public key of a private key/public key pair of the trusted body~~ recording the encrypted messages, and using the recorded dialogue together with the confidential record of the relation between the identity of a user and the random identifier to provide a means of non-repudiation of the dialogue by users.

18. (Previously Presented) A method according to Claim 1, wherein the trusted body maintains the private key of said private key/public key pair, and the step of using said private key to decrypt the encrypted messages.

19. (New) A method according to Claim 1, wherein:

the user has a third public/private key pair;

the steps of sending the public key of the public/private key pair to the trusted body includes the steps of the user signing the first public key by using the third private key and sending the signed first public key to the trusted body;

comprising the further steps of:

the trusted body verifying the identify of the user by obtaining the third public key and using the third public key to verify the signature of the user on the first public key;

the trusted body, after verifying the identify of the user, signing the random identifier and sending the signed random identifier to the user; and

the user signing the message with the random identifier.